TRACCIA 1

Use the attached dossier to write a report for a newly-appointed workgroup of MEPs (Members of the European Parliament) giving an overview of cyber security in Italy. It is to be assumed that the readers may have little prior knowledge of this issue. The report should follow the conventional layout for this type of document in English and should not exceed one thousand words.

Ho estratto questa traccia

From the ACN Website:

L'Agenzia è stata istituita dal Decreto-legge n.82 del 14 giugno 2021 che ha ridefinito l'architettura nazionale di cybersicurezza, con l'obiettivo di razionalizzare e semplificare il sistema di competenze esistenti a livello nazionale, valorizzando ulteriormente gli aspetti di sicurezza e resilienza cibernetiche, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico.

L'Agenzia per la cybersicurezza nazionale (ACN) è l'Autorità nazionale per la cybersicurezza a tutela degli interessi nazionali nel campo della cybersicurezza. L'Agenzia ha il compito di tutelare la sicurezza e la resilienza nello spazio cibernetico. Si occupa di prevenire e mitigare il maggior numero di attacchi cibernetici e di favorire il raggiungimento dell'autonomia tecnologica. Tra i principali compiti dell'Agenzia c'è l'attuazione della Strategia Nazionale di Cybersicurezza, adottata dal Presidente del Consiglio, che contiene gli obiettivi da perseguire entro il 2026.

In un mondo sempre più digitalizzato e connesso, la cybersicurezza è diventata di fondamentale importanza. Per questo è nata la **Strategia Nazionale di Cybersicurezza** volta a pianificare, coordinare e attuare misure tese a **rendere il Paese più sicuro e resiliente.**

La strategia prevede il raggiungimento di **82 misure entro il 2026**. Un percorso all'insegna dell'innovazione definito dall'Agenzia per la cybersicurezza nazionale, che si occuperà anche di controllare che gli obiettivi vengano raggiunti. *

(Alcuni uffici e mansioni del ACN)

Regolazione

Svolge le attività regolatorie e attuative della vigente disciplina in materia di cybersicurezza, sia di derivazione comunitaria che nazionale, garantendone il rispetto anche attraverso l'esercizio dei poteri sanzionatori. Coordina, altresì, le attività esercitative che simulano eventi e crisi di natura cibernetica.

Certificazione e vigilanza

Valuta prodotti e servizi informatici e conduce attività ispettive e di verifica rispetto agli adempimenti normativi nel campo della cybersicurezza. Al suo interno è costituito il Centro di Valutazione e Certificazione Nazionale (CVCN). Esercita le funzioni di Autorità Nazionale di Certificazione della Cybersicurezza (NCCA).

Operazioni e gestione delle crisi cyber

Si occupa delle attività di prevenzione, monitoraggio, analisi e risposta agli eventi di natura cibernetica, all'interno della quale opera il CSIRT - Computer Security Incident Response Team - Italia

Programmi industriali, tecnologici e di ricerca

Svolge funzioni di indirizzo e gestione delle attività svolte dall'Agenzia per promuovere l'autonomia strategica e la sovranità tecnologica nazionale. Supporta l'attuazione della Strategia Nazionale di Cybersicurezza e ha responsabilità nella gestione dell'investimento 1.5 " Cybersecurity" del PNRR.
Progetta e implementa i sistemi e gli applicativi a supporto dell'Agenzia e dei servizi cyber nazionali. Gestisce e coordina le iniziative progettuali di ricerca in ambito cyber. È punto contatto nazionale, verso il Centro Europeo di Competenza per la Cybersicurezza (ECCC), della rete degli NCC e la Community.

Strategie e Cooperazione

Definisce gli indirizzi strategici e gli strumenti di policy nazionali in materia di cybersicurezza, ne monitora l'attuazione, nonché mantiene e sviluppa le relazioni e la cooperazione internazionale dell'Agenzia.

Formazione e consapevolezza

La promozione delle competenze di cybersicurezza nel Paese è tra le priorità dell'Agenzia, allo scopo di accrescere qualità e numero degli esperti di settore, ampliare le conoscenze in ambito cyber dei professionisti e rendere i cittadini più consapevoli delle opportunità e dei rischi della vita digitale.

*Nota in merito alla Misura #82

La **Misura #82** della Strategia Nazionale di Cybersicurezza 2022-2026 dell'Italia è dedicata alla definizione e all'implementazione di metriche e Key Performance Indicators (KPI) per monitorare l'attuazione delle misure previste dalla strategia stessa. Il "Manuale operativo - Attuazione misura #82" specifica tali metriche e indicatori per ciascuna delle 82 misure delineate nel piano di implementazione.

Per ogni misura, il manuale dettaglia:

- **Metriche**: Parametri specifici utilizzati per quantificare gli aspetti chiave dell'attuazione della misura.

- **Indicatori**: Valori numerici o qualitativi che riflettono il progresso o il successo nell'implementazione della misura.
- **Affidabilità**: Livello di precisione e oggettività dell'indicatore, classificato come "medio" o "alto".
- **Anno di implementazione prevalente**: L'anno in cui si prevede principalmente l'attuazione della misura.
- **Linee guida per la misurazione**: Indicazioni su come raccogliere e interpretare i dati relativi agli indicatori.

In totale, il manuale identifica 261 indicatori associati alle 82 misure. Questi KPI coprono vari ambiti, tra cui:

- **Protezione**: Misure per salvaguardare le infrastrutture critiche e i dati sensibili.
- **Risposta**: Capacità di affrontare e mitigare incidenti e crisi cibernetiche.
- **Sviluppo**: Promozione di tecnologie sicure e potenziamento delle competenze nel settore della cybersicurezza.

Adapted from:

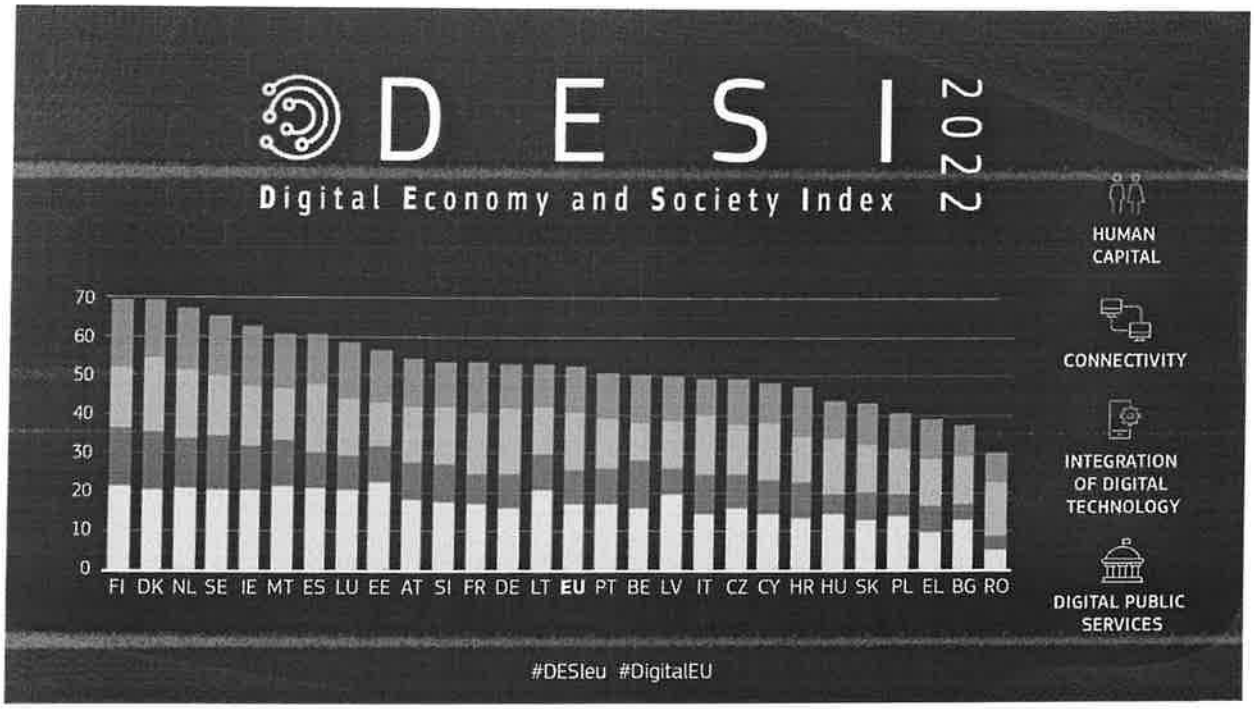
https://www.cybersecurity360.it/soluzioni-aziendali/mancanza-di-competenze-cyber-in-italia-come-risolvere-il-problema/

Mancanza di competenze cyber in Italia: come risolvere il problema

L'Italia affronta una carenza significativa di competenze nella cybersecurity, con la necessità urgente di potenziare la formazione e la consapevolezza per proteggere aziende e istituzioni dalle minacce digitali. Partner affidabili e una formazione continua sono essenziali per garantire la sicurezza e la resilienza dei sistemi informativi

Pubblicato il 9 ago 2024
Marco R. A. Bozzetti - Presidente AIPSI
Gianluca Lombardi - Ingegnere, Maestro della Privacy, DPO, Auditor Privacy, Socio Clusit, Ceo di GL Consulting

L'Italia si trova in una posizione arretrata rispetto agli altri paesi europei per quanto riguarda le competenze digitali. Secondo l'indice di **Digitalizzazione dell'economia e della società (DESI)**, l'Italia è tra gli ultimi posti nell'UE per competenze digitali.



"L'Italia deve far fronte a notevoli carenze nelle competenze digitali di base e avanzate, che rischiano di tradursi nell'esclusione digitale di una parte significativa della popolazione e di limitare la capacità di innovazione delle imprese" sottolinea il rapporto.

In particolare, la mancanza di specialisti nella cibersicurezza è una sfida critica. Le competenze richieste per ruoli specifici in questo settore, come ad esempio i 12 profili

descritti in **ECSF di ENISA***, non sono facilmente reperibili, creando un vuoto significativo nella difesa non solo delle infrastrutture critiche nazionali, ma di tutti i sistemi informativi, piccoli o grandi, di ogni azienda in ogni settore merceologico, oltre che delle pubbliche amministrazioni centrali e locali.

Negli ultimi anni, l'Italia ha visto un aumento significativo sia nel numero che nella gravità degli attacchi informatici. I rapporti più recenti dell'**Agenzia per la Cybersecurity Nazionale (ACN)** e dell'**Osservatorio Attacchi Digitali (OAD)** evidenziano un incremento preoccupante di incidenti, con attacchi sempre più sofisticati e mirati.

Questa critica tendenza evidenzia la necessità urgente di migliorare e potenziare la cibersicurezza dei sistemi informativi, e questo richiede competenze idonee da parte degli utenti, finali o privilegiati, che da sempre costituiscono l'anello più vulnerabile della sicurezza digitale, e anche una adeguata conoscenza del problema da parte dei "decision maker" che stabiliscono budget e priorità.

La realtà delle microimprese italiane

Secondo il **Rapporto sulle Imprese 2021** di ISTAT, in Italia il 95% delle imprese ha meno di 10 dipendenti.

Queste microimprese, a parte quelle del mondo ICT, non possono avere e mantenere al proprio interno personale specializzato in ICT e, ancora meno, nella cibersicurezza: devono quindi rivolgersi e fare affidamento su consulenti esterni o società specializzate in tali ambiti.

La cybersicurezza è, inoltre, basilare per garantire la conformità a varie normative vigenti o da attuare a breve, come ad esempio il **GDPR**, la **direttiva NIS 2** e il regolamento **DORA**.

La non conformità può comportare sanzioni significative e danni reputazionali, rendendo imprescindibile una formazione adeguata e continua dei leader aziendali in materia di cyber security e governance.

Conclusione

Potenziare e migliorare il livello di cibersicurezza significa in primo luogo meglio sensibilizzare e formare gli utenti a tutti i livelli.

* L'**European Cybersecurity Skills Framework (ECSF)**, sviluppato dall'Agenzia dell'Unione Europea per la Cybersicurezza (ENISA), identifica **12 profili professionali tipici nel settore della cybersicurezza**. Ciascun profilo è dettagliato con missioni, compiti, competenze, abilità e conoscenze specifiche:

1. **Chief Information Security Officer (CISO)**: Gestisce la strategia di cybersicurezza dell'organizzazione, assicurando che i sistemi digitali, i servizi e gli asset siano adeguatamente protetti.

2. **Cyber Incident Responder**: Monitora lo stato di cybersicurezza dell'organizzazione, gestisce gli incidenti durante gli attacchi informatici e garantisce la continuità operativa dei sistemi ICT.

3. **Cyber Legal, Policy and Compliance Officer**: Supervisiona e garantisce la conformità con i framework legali e regolamentari relativi alla cybersicurezza e alla protezione dei dati, in linea con la strategia dell'organizzazione.

4. **Cyber Threat Intelligence Specialist**: Analizza e monitora le tattiche, le tecniche e le procedure utilizzate dagli attori delle minacce cibernetiche, tracciando le loro attività e valutando le tendenze.

5. **Cybersecurity Architect**: Pianifica e progetta soluzioni basate su principi di sicurezza fin dalla progettazione, sviluppando modelli architetturali e specifiche per garantire la sicurezza dei sistemi.

6. **Cybersecurity Auditor**: Conduce revisioni indipendenti per valutare l'efficacia dei processi e dei controlli, assicurando la conformità complessiva con i framework legali e regolamentari dell'organizzazione.

7. **Cybersecurity Educator**: Migliora le conoscenze, le abilità e le competenze in materia di cybersicurezza attraverso la progettazione, lo sviluppo e l'erogazione di programmi di sensibilizzazione, formazione ed educazione.

8. **Cybersecurity Implementer**: Sviluppa, distribuisce e gestisce soluzioni di cybersicurezza (sistemi, asset, software, controlli e servizi) su infrastrutture e prodotti, garantendo la loro efficacia operativa.

9. **Cybersecurity Researcher**: Conduce ricerche nel dominio della cybersicurezza e integra i risultati nelle soluzioni di sicurezza, contribuendo all'innovazione e all'avanzamento del settore.

10. **Cybersecurity Risk Manager**: Gestisce i rischi legati alla cybersicurezza dell'organizzazione, sviluppando, mantenendo e comunicando processi di gestione del rischio allineati alla strategia aziendale.

11. **Digital Forensics Investigator**: Assicura che le indagini su crimini informatici rivelino tutte le prove digitali necessarie per dimostrare attività malevole, attraverso la raccolta, l'analisi e la conservazione dei dati.

12. **Penetration Tester**: Valuta l'efficacia dei controlli di sicurezza, identificando e sfruttando le vulnerabilità per determinare la loro criticità se utilizzate da attori malevoli.

Source: Il Messaggero

Dati rubati, l'esperto: «La cybersecurity è un settore grigio. Con una talpa impossibile difendersi»

Quando si parla di cybersecurity, «la manipolazione dell'essere umano è ancora l'attacco più efficace di tutti». E, nel caso di dipendenti infedeli, «non c'è sistema informatico che tenga» e difendersi da episodi del genere «sarà sempre più difficile». Ne è convinto Alessandro Curioni, esperto di cybersecurity, docente del corso di Sicurezza dell'informazione alla Cattolica di Milano e fondatore di DI.GI Academy, azienda specializzata in sicurezza informatica. Nell'ordinanza di custodia cautelare viene menzionata la possibilità che siano stati scaricati dati direttamente dalla banca dati Sdi del Ministero dell'Interno. Come ci sarebbero riusciti

«Avevano qualcuno all'interno. Dalle notizie emerse finora si parla di complici nelle Forze dell'Ordine e di infiltrati tra i fornitori che si occupano della manutenzione dei sistemi. Così, mi lasci dire, è proprio facile».

Serve necessariamente avere un uomo all'interno per operazioni del genere?

«Non sempre, in passato ci sono riusciti anche senza averne uno ma ci vogliono competenze straordinarie in campo informatico. E bisogna investirci sopra una quantità massiccia di tempo e di denaro. È il caso degli attacchi state-sponsored (attacchi informatici effettuati da uno stato-nazione contro un altro governo, ndr), che lavorano per anni su un preciso target con attacchi sofisticati alla ricerca di una vulnerabilità tecnologica da sfruttare».

Ma non è questo il caso.

«Qui parliamo di crimine con finalità di lucro e profitto, e questo tipo di crimine segue sempre la via più facile. Non servono attacchi informatici particolarmente complicati: basta promettere a qualcuno una fetta dei guadagni e, se è abbastanza grossa, la tentazione farà il resto».

Si parla anche della clonazione di un indirizzo email assegnato al Presidente della Repubblica.

«Probabilmente è stato creato un falso account a nome del Presidente della Repubblica con il quale sono state inviate delle email. Falsificare un account non è particolarmente difficile, spesso basta modificare una singola lettera nel dominio della casella».

Che fine fanno i dati sottratti?

«Parliamo sempre di furti su commissione, magari per sapere qualcosa di più su un concorrente, su un dipendente potenzialmente infedele, su un socio o su un parente, perché magari c'è di mezzo un'eredità. I dati vengono rivenduti, dietro c'è un mercato importante».

È una pratica diffusa all'interno della Pa?

«Credo che il settore della cybersecurity sia un settore grigio. Ci sono delle pratiche che sono decisamente borderline, ed è un attimo prima che quel grigio diventi tutto nero. Il caso Telecom di qualche anno fa non era poi tanto diverso da questo. Tragga lei le conclusioni».

Quanto è indietro il nostro sistema normativo rispetto all'avanzamento tecnologico?

«Secondo me non è una questione tecnologica. Non concordo con Nordio quando dice che "dobbiamo essere al loro passo". Io posso mettere tutte le misure di sicurezza che voglio, cifratura, autenticazioni multiple... Ma se la persona che entra nei sistemi era infedele, e ha tutte le password per accedere a quei dati, l'unica possibilità che ho è un controllo. Molto rigido e molto rigoroso. Però attenzione, perché in Italia la normativa sul diritto del lavoro rende molto difficile monitorare le attività dei dipendenti».

Prima parlava di attacchi state-sponsored. I nostri sistemi sarebbero in grado di difendersi?

«Non credo. Nessuna nazione sarebbe in grado di difendersi da un attacco del genere».

E da attacchi come questo, dove invece viene sfruttata la variabile umana?

«Consideri che le tecniche di ingegneria sociale sono di gran lunga le più efficaci e le più efficienti, anche in presenza di una vulnerabilità. Se non iniziamo ad aggiustare le cose partendo dalla formazione e dalla diffusione di una cultura informatica adeguata, difendersi da situazioni come questa sarà sempre più difficile».

Raffaele D'Ettorre

Lunedì 28 Ottobre 2024, 06:23 - Ultimo aggiornamento: 29 Ottobre, 08:39

PA GAZZETTA

"La Cybersicurezza in Italia: Parla l'Esperto"

Nell'era della digitalizzazione, la cybersicurezza è diventata una priorità per governi, aziende e cittadini. Abbiamo intervistato la dottoressa Maria Rossi, esperta di sicurezza informatica, per comprendere meglio le sfide e le strategie attuali in Italia.

Giornalista: Dottoressa Rossi, può illustrare un quadro della situazione attuale della cybersicurezza in Italia?

Dott.ssa Rossi: Certamente. L'Italia, come molti altri paesi, sta affrontando un periodo critico dal punto di vista della cybersicurezza. La pandemia di COVID-19 ha accelerato la trasformazione digitale in molti settori, dalla pubblica amministrazione alla sanità, ma purtroppo non tutti erano pronti a gestire le nuove sfide di sicurezza. Abbiamo assistito a un aumento significativo di attacchi informatici, in particolare ransomware, phishing e attacchi a infrastrutture critiche.

Solo nel 2022, secondo i dati dell'ACN, gli attacchi ransomware hanno colpito numerose aziende e anche enti pubblici, compromettendo servizi essenziali. In un contesto come quello italiano, dove le piccole e medie imprese (PMI) costituiscono il tessuto economico principale, il problema è amplificato: molte di queste realtà non dispongono di risorse adeguate per implementare solide difese informatiche.

Giornalista: Quali sono le principali minacce che l'Italia deve affrontare in questo momento?

Dott.ssa Rossi: Le minacce sono molteplici e in continua evoluzione. Il ransomware è sicuramente una delle più frequenti, con i criminali che bloccano i sistemi e chiedono un riscatto per ripristinarli. Gli attacchi DDoS (Distributed Denial-of-Service), che inonda un server di traffico Internet per impedire agli utenti di accedere ai servizi e ai siti online collegati, sono altrettanto diffusi, così come il furto di dati personali e sensibili.

Particolarmente preoccupanti sono gli attacchi alle infrastrutture critiche, come reti energetiche, ospedali e trasporti. Questi settori sono ormai strettamente interconnessi attraverso tecnologie digitali, il che aumenta il rischio di incidenti con ripercussioni gravi non solo dal punto di vista economico, ma anche sociale.

Giornalista: Quali misure sta adottando l'Italia per affrontare queste sfide?

Dott.ssa Rossi: Negli ultimi anni, il governo italiano ha fatto passi avanti significativi. L'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN) nel 2021 è stata una svolta importante. L'agenzia coordina le attività di prevenzione e risposta agli attacchi, lavorando in stretta collaborazione con aziende private, istituzioni pubbliche e partner internazionali.

Inoltre, è stata definita una Strategia Nazionale di Cybersicurezza per il periodo 2022-2026, che punta su vari aspetti: rafforzare la protezione delle infrastrutture critiche, sviluppare competenze specializzate, promuovere la collaborazione tra pubblico e privato e migliorare la resilienza complessiva del sistema.

Giornalista: Quali sono, però, le sfide ancora aperte?

Dott.ssa Rossi: Una delle principali sfide è la mancanza di competenze specializzate. Si stima che in Italia ci sia un divario significativo tra la domanda e l'offerta di esperti in cybersicurezza. Questo problema non riguarda solo il settore pubblico, ma anche le PMI, che spesso non hanno risorse sufficienti per assumere specialisti.

Un'altra difficoltà è la scarsa consapevolezza del rischio. Troppo spesso le aziende e i cittadini sottovalutano l'importanza della sicurezza informatica. Pensiamo, ad esempio, all'uso di password deboli o alla mancanza di aggiornamenti nei sistemi. È fondamentale investire in formazione e sensibilizzazione, anche a livello di scuole e università.

Giornalista: Qual è il ruolo dell'Italia nel contesto internazionale della cybersicurezza?

Dott.ssa Rossi: L'Italia gioca un ruolo importante, collaborando con l'Unione Europea e la NATO. Siamo coinvolti in programmi di ricerca e sviluppo tecnologico, come Horizon Europe, e lavoriamo con i nostri partner per affrontare minacce globali. La cybersicurezza è un tema senza confini, e la cooperazione internazionale è essenziale per proteggere infrastrutture e cittadini.

Giornalista: Guardando al futuro, cosa possiamo aspettarci?

Dott.ssa Rossi: Credo che nei prossimi anni vedremo un aumento degli investimenti in tecnologie innovative come intelligenza artificiale e blockchain, che possono migliorare significativamente la sicurezza informatica. Inoltre, la formazione di professionisti qualificati e una maggiore sensibilizzazione a tutti i livelli saranno fondamentali.

Quello che è certo è che la cybersicurezza deve diventare una priorità non solo per le istituzioni, ma per tutta la società. Solo così potremo affrontare le sfide di un mondo sempre più digitale in modo efficace e sicuro.

Giornalista: Grazie per il suo tempo e le preziose informazioni, dottoressa Rossi.

Dott.ssa Rossi: Grazie a voi per l'attenzione a un tema così cruciale.

Source: Sito web Minint

Investimento 1.5 " Cybersecurity" del PNRR – Ministero dell'Interno

M1C1 Investimento 1.5: Cybersecurity

Importo: euro € 67.250.000

L'investimento è diretto a rafforzare le difese informatiche del Paese, con specifica attenzione alla Pubblica Amministrazione

Amministrazione titolare dell'Investimento è il Ministero per l'Innovazione Tecnologica e la Transizione Digitale.

Soggetto attuatore dell'investimento: Agenzia per la Cybersicurezza Nazionale.

Amministrazione attuatrice del progetto: Direzione Centrale per la Polizia Stradale, Ferroviaria, delle Comunicazioni e per i Reparti Speciali della Polizia di Stato – Servizio Polizia Postale e delle Comunicazioni.

La finalità dell'Investimento 1.5 è quella di rafforzare le difese cibernetiche, aumentando il grado di resilienza informatica del Paese, con specifico riferimento al settore della Pubblica Amministrazione, anche per poter fronteggiare sempre più efficacemente la continua evoluzione della minaccia cyber. Ciò anche attraverso la capacità di prevedere o rilevare tempestivamente attacchi e incidenti informatici, reagire e ripartire in tempi rapidi, minimizzando i danni.

Gli investimenti strategici in tema di Cybersecurity a cura del Dipartimento della Pubblica scurezza sono:

a) "C-LABS", che prevede la realizzazione di 28 laboratori per l'analisi forense, presso i Compartimenti, le Sezioni Distrettuali ed il CNAIPIC (Polizia Postale) – finanziamento di 29.000.000 euro;

b) realizzazione del Centro di valutazione C.V. del Ministero dell'Interno, previsto in seno al CERT di prossima istituzione (Polizia Postale) – finanziamento di 9.250.000 euro;

c) realizzazione del Security Operation Center - S.O.C. del Dipartimento della Pubblica sicurezza (Direzione Centrale dei Servizi Tecnico Logistici e della Gestione Patrimoniale) – finanziamento di 29.000.000 euro

Adapted from Wired

Il gap di competenze (e di professionisti) in cybersicurezza si affronta facendo cultura

La sensibilizzazione sul tema della cybersecurity, con la formazione di nuove professionalità mirate, è essenziale per la trasformazione digitale e per ridurre il rischio di attacchi: Microsoft promuove nuovi percorsi gratuiti per contribuire a colmare l'attuale gap, di competenze e nel mercato del lavoro

Nel mondo la domanda di **lavoratori e specialisti della cybersicurezza** è altissima: sono ricercati **più di 3,4 milioni i profili**, e solo in Italia si stima una carenza di circa **100mila professionisti** della sicurezza informatica. D'altronde, se tutto ciò che viaggia attraverso la rete dev'essere controllato e monitorato, è necessario che tutti (inclusi soprattutto i non addetti ai lavori) siano consapevoli dei **rischi** e dei **pericoli** che si corrono quotidianamente. Per questo motivo, figure come **data scientist**, **chief information security officer** (i cosiddetti Ciso) e **IoT software engineer** sono ora essenziali nel contesto aziendale, perché agevolano il processo di transizione digitale e offrono garanzie sul corretto funzionamento dei sistemi di sicurezza. E allo stesso tempo **la cybersecurity è diventata una questione collettiva**, che riguarda di fatto chiunque utilizzi i device e la rete.

L'impegno per formare nuove professionalità

Un progetto formativo targato Microsoft mira da un lato a rafforzare le difese dai cyberattacchi grazie all'utilizzo di **software intelligenti** e all'analisi delle enormi quantità di dati a

disposizione, mentre dall'altro lato promuove lo sviluppo di **percorsi formativi** per colmare i già citati gap di competenze.

I corsi, accessibili attraverso la piattaforma della Fondazione Mondo Digitale, offrono brevi video-pillole su argomenti che spaziano dall'**uso di password efficaci** alla comprensione dei principali rischi online e alle pratiche per effettuare **transazioni sicure**.

L'AI, la cybersicurezza e le aziende

Il più recente Digital Defense Report rivela che la sola Microsoft raccoglie oltre **65mila miliardi di segnali d'attacco ogni giorno**. Con un aumento globale delle azioni malevole che hanno interessato 120 Paesi, è emerso anche un trend crescente sullo **spionaggio governativo**. In un contesto in cui gli attacchi informatici evolvono, emergono come principali attività dei cybercriminali il **furto di informazioni**, il **monitoraggio delle comunicazioni** e la **manipolazione delle informazioni**.

"Rischi e minacce stanno crescendo costantemente. La mancanza di competenze adeguate nel settore della cybersecurity – sia avanzate sia di base – può causare danni significativi non solo alle aziende ma a tutti noi", ha spiegato **Tamara Zancan**, Direttrice Cybersecurity, Compliance e Identity di Microsoft Italia. "***Non è più una questione per i soli addetti ai lavori***, *ma è necessario che tutti prestino attenzione alla sicurezza dei propri dati, per se stessi e per gli altri. Il rischio non riguarda solamente* ***le grandi aziende***, *ma anche per* ***le piccole e medie imprese*** *e* ***i singoli cittadini***".

Non a caso, la **formazione del capitale umano** è oggi un elemento urgente per prevenire e rispondere alle minacce in maniera efficace e trasversale. E si torna ancora una volta al tema dei disallineamenti nel mercato del lavoro: secondo il report Cybersecurity Ventures, i posti vacanti nel settore della sicurezza informatica **sono aumentati del 350% dal 2013 a oggi**.

Gianluca Dotti

Adapted from US government site - https://www.trade.gov/country-commercial-guides/italy-cybersecurity

Overview

In 2022, the cybersecurity market was valued at $2.1 billion, 18% more than the previous year. Italy continues to rank fourth in the world and first in Europe for the number of cyberattacks. With the growth in remote work, attacks on PCs doubled, as cyber criminals shifted their focus to the weakest link in the chain: the endpoint and the employee's PC. Ransomware threats have the greatest impact, increasingly targeting the manufacturing sector, the public administration, and healthcare facilities. According to the Italian Cybersecurity Association (CLUSIT), in 2022, the Postal and Communications Police (CNAIPIC) managed nearly 13,000 significant cyberattacks, more than twice the number in the previous year. CNAIPIC mostly engages when malware attacks, especially ransomware attacks, phishing, distributed denial-of-service (DDos) attacks, and advanced persistent threat (APT) campaigns are involved. There were over 113,000 security alerts involving IT services of institutions, critical IT infrastructures of national interest, sensitive infrastructure of regional interest, banks, and large companies operating in strategic sectors such as communications and defense. Russia's war against Ukraine and the ensuing financial and energy crisis generated an unprecedented surge in cyberattacks, particularly DDoS attacks, which increased exponentially last year. Many attacks are traceable to Chinese and Russian hacking groups that operate transnationally.

Leading Sub-Sectors

Significantly more malware families were detected in 2022 (208) than in 2021 (163). Infection penetration has also become relevant in mobile, with the FluBot malware infecting mainly Android devices. The primary sectors targeted include finance, insurance, and public administration. Larger companies turned to tools such as firewalls or virtual private networks (VPN) to raise protection levels, providing employees with remote access to corporate VPNs while augmenting perimeter protection.

More than 50% of SMEs are unprepared to face increasing threats. One in five companies lack a specific investment plan for IT security or only allocate resources as needed. However, medium-sized companies and (to a lesser extent) small companies are increasingly choosing to invest in cybersecurity, often opting for advanced cloud security solutions.

Opportunities

Cybersecurity is a key element in Italy's digital transformation strategy. Government measures are being put in place to boost efforts to counter cyber risks. The National Cybersecurity Authority (ACN) was established in June 2021 to protect the national cyberspace. The agency promotes a coherent regulatory framework in the sector and exercises inspection and sanction functions. ACN ensures the implementation of Italy's first-ever **cybersecurity**

strategy announced in May 2022, which outlines the country's digital roadmap. Security and innovation are priorities of the plan, which seeks to implement over 80 measures by 2026, some via public-private partnership. The goal is to have 75% of the Italian administration migrated to cloud services by 2026.

The National Cybersecurity Perimeter Law ensures a high level of security for networks, IT systems, and services used by government agencies, public administration, state-owned entities, and private companies that exercise an essential function of the state or services fundamental to the country's interests and national security. It also provides the framework for providers of IT products and services that must meet certain requirements, such as data localization. The law also provides a legislative amendment on foreign investments in certain strategic sectors.